MAXLOOP

Smart Contract Security Assassment

Quick Check

Disclaimer

Maxloop Blockchain Security (Maxloop) has conducted an independent audit to verify the integrity of and highlight any vulnerabilities or errors, intentional or unintentional, that may be present in the codes that were provided for the scope of this audit. This audit report does not constitute agreement, acceptance or advocation for the Project that was audited, and users relying on this audit report should not consider this as having any merit for financial advice in any shape, form or nature. The contracts audited do not account for any economic developments that may be pursued by the Project in question, and that the veracity of the findings thus presented in this report relate solely to the proficiency, competence, aptitude and discretion of our independent auditors, who make no guarantees nor assurance that the contracts are completely free of exploits, bugs, vulnerabilities or deprecation of technologies. Further, this audit report shall not be disclosed nor transmitted to any persons or parties on any objective, goal or justification without due written assent, acquiescence or approval by Maxloop.

All information provided in this report does not constitute financial or investment advice, nor should it be used to signal that any persons reading this report should invest their funds without sufficient individual due diligence regardless of the findings presented in this report. Information is provided 'as is', and Maxloop is under no covenant to the completeness, accuracy or solidity of the contracts audited. In no event will Maxloop or its partners, employees, agents or parties related to the provision of this audit report be liable to any parties for, or lack thereof, decisions and/or actions with regards to the information provided in this audit report.

Cryptocurrencies and any technologies by extension directly or indirectly related to cryptocurrencies are highly volatile and speculative by nature. All reasonable due diligence and safeguards may yet be insufficient, and users should exercise considerable caution when participating in any shape or form in this nascent industry.

The audit report has made all reasonable attempts to provide clear and articulate recommendations to the Project team with respect to the rectification, amendment and/or revision of any highlighted issues, vulnerabilities or exploits within the contracts provided. It is the sole responsibility of the Project team to sufficiently test and perform checks, ensuring that the contracts are functioning as intended, specifically that the functions therein contained within said contracts have the desired intended effects, functionalities and outcomes of the Project team.

1 Overview

This free report has been prepared for Wrapped NewYorkCoin on the Binance Smart Chain (BSC). Maxloop provides a user-centred examination of the smart contracts to look for vulnerabilities, logic errors or other issues from both an internal and external perspective.

1.1 Summary

Project Name	Wrapped NewYorkCoin
URL	https://wrappednyc.com/
Platform	Binance Smart Chain
Language	Solidity

1.2   Contracts Assessed

Name	Contract	Live Code Match
Wrapped NewYorkCoin	0x6c015277b0f9b8c24b20bd8bbbd29fdb25738a69	✓ MATCH
Wrapped NewYorkCoin.sol	0x1f2952769ED1ce42fFe57274fF44D155D74C8e1e	✓ MATCH

1.3   Findings Summary

Severity	Found	Resolved	Partially Resolved	Acknowledged (no change made)
🔴 High	0	-	-	-
🟠 Medium	0	-	-	-
🟡 Low	3	1	-	2
🟢 Informational	1	-	-	1
Total	**4**	**1**	**-**	**3**

Classification of Issues

Severity	Description
🔴 High	Exploits, vulnerabilities or errors that will certainly or probabilistically lead towards loss of funds, control, or impairment of the contract and its functions. Issues under this classification are recommended to be fixed with utmost urgency.
🟠 Medium	Bugs or issues with that may be subject to exploit, though their impact is somewhat limited. Issues under this classification are recommended to be fixed as soon as possible.
🟡 Low	Effects are minimal in isolation and do not pose a significant danger to the project or its users. Issues under this classification are recommended to be fixed nonetheless.
🟣 Informational	Consistency, syntax or style best practices. Generally pose a negligible level of risk, if any.

1.4 Wrapped NewYorkCoin

ID	Severity	Summary	Status
01	LOW	Mint function can be used to pre-mint large amounts of tokens before Ownership is transferred to the **Masterchef**	● RESOLVED

1.5 Wrapped NewYorkCoin Severity

ID	Severity	Summary	Status
01	LOW	Inconsistency between deposit fee cap in add and set	ACKNOWLEDGED
02	LOW	PendingMondo will show inaccurate pending harvests on the dapp frontend If the pending rewards causes totalSupply to be exceed **MAXSUPPLYCAP**	ACKNOWLEDGED
03	INFO	Total token supply might not be minted due to try and catch pattern	ACKNOWLEDGED